Билет 6

Опр. числа $a_1, \dots a_n \in \mathbb{Z}$ называются взаимно простыми, если $(a_1, \dots a_n) = 1$

Если любые 2 из $a_1, \dots a_n$ взаимно просты, эти числа называют попарно взаимно простыми // $(a_i, \dots a_j)$ – НОД $a_i, \dots a_j$

Свойства:

- 1) Если $a_1, \dots a_n \in \mathbb{Z}$ попарно взаимно просты, то они взаимно просты.
  ▷ Если $(a_1, \dots a_n) = d > 1$, то $(a_1, a_2) \vdots d$, значит $(a_1, a_2) > 1$ (!!!) ◁
- 2) Если $a, b, c \in \mathbb{Z}$ и $(a, b) = 1$, то $(ac, b) = (c, b)$.
  ▷ $\exists\, d = (c, b)$, $f = (ac, b)$. Из $c \vdots d$ следует, что $ac \vdots d$. Значит $d \in OD(ac, b)$ (множество всех общих делителей (ac, b)) и по теореме о НОД $f \vdots d$. Из $b \vdots f$ следует, что $bc \vdots f$ (домножили). Тогда $f \in OD(ac, bc)$, $f \vdots$ т.к. 2. Тогда по теореме 3 $c = c(a, b) = (ac, bc) \vdots f$ ($(a, b) = 1$). Тогда $f \in OD(c, b)$ и по т.к. 2 $d \vdots f$. Т.к. $d, f \in \mathbb{N}$, $d \vdots f$, $f \vdots d \Rightarrow d = f$. ◁
- 3) Если $a, b, c \in \mathbb{Z}$, $(a, b) = 1$ и $ac \vdots b$, то $c \vdots b$. // как бы продолжение свва 2
  ▷ По свву 2 $(c, b) = (ac, b) = b \Rightarrow c \vdots b$ ◁ ($(a, b) = 1$, т.к. $ac \vdots b$)
- 4) $\exists\, a_1, \dots a_n, b_1, \dots b_m \in \mathbb{Z}$, причём $(a_i, b_j) = 1$ для $\forall i \in \{1, \dots n\}, j \in \{1, \dots m\}$. Тогда $(a_1, \dots a_n, b_1, \dots b_m) = 1$ // перемножили
  ▷ Докажем по индукции: $(a_1 \dots a_k, b_j) = 1$ для всех $j \in \{1, \dots m\}$ и $k \in \{1, \dots n\}$ индукция по k. База очевидна. Переход $k \to k+1$: $(a_1, a_k a_{k+1}, b_j) = (a_1, \dots a_k, b_j) = 1$, по свву о $(a_{k+1}, b_j) = 1$ // свва 2

// Кратко о свойствах: 1 и 4 похожи, о попарном сравнении, 2 о домножении, 3 о домножении на делящееся.

Билет 7

Опр. натуральное число, имеющее ровно 2 натуральных делителя, называют простым. $\{2, 3, 5, 7, 11 \dots\}$

Опр. натуральное число с больш. кол-вом делителей – составное.

$1 \in \mathbb{P}$. $\forall p \in \mathbb{P}$, кол-во всех его делителей: 1 и p. $\{4, 6, 8, 9 \dots\}$

Опр. $\exists\, a \in \mathbb{N}$. Собственный делитель числа a – любой его делитель, отличный от 1. $6 = 2 \cdot 3$, $2 \neq 1$, $6 \vdots 2 \Rightarrow 2$ – собств. делитель a (как и 3)

Свойства:

- 1) $\exists\, a \in \mathbb{N}$ – составное, тогда $\exists$ разложение $a = bc$, где $b, c \in \mathbb{N}$, $a > b$, $c > 1$.
  ▷ Составное число имеет собственный делитель $b < a$. Тогда $a = bc$, где $c \in \mathbb{N}$, $1 < c < a$ – очевидно. ◁

• 2) ∃ $a \in \mathbb{N}$, $a \neq 1$, а d - минимальный собственный делитель a. Тогда $d \in \mathbb{P}$.
т.к. определили, как составное
▷ $d > 1$ - по определению. ∃ d - составное. По свву 1 $d = bc$, где $d > b > 1$, но из ~~$d:d$~~ $d:b, a:d$ следует, что $a:b$, значит $b < d$ - собственный делитель a, противоречие с выбором d в качестве минимального. ◀

• 3) ∃ $a \in \mathbb{Z}$, $p \in \mathbb{P}$. Тогда либо $a:p$, либо $(a,p) = 1$.
▷ Так как $d = (a,p) \in \mathbb{N}$ и $p:d$, то $d = 1$ или $d = p$ // по опр. простого числа
Если $(a,p) = p$, то $a:p$. ◀

• 4) ∃ $a_1, \dots a_n \in \mathbb{Z}$ и $p \in \mathbb{P}$ таковы, что $a_1 \cdot \dots a_n : p$. Тогда ∃ такое $i \in \{1, \dots n\}$, то $a_i : p$. // найдётся какое-то делящееся
▷ ∃ $a_i \not: p$ для всех $i \in \{1, \dots n\}$. Тогда по свву 3 (либо p, либо 1) $(a_i, p) = 1$. Но по свву 4 взаимно простых чисел, $(a_1 \cdot \dots a_n, p) = 1$, тогда и $a_1 \cdot \dots a_n \not: p$. Противоречие (!!!) ◀

Теорема 6

Простых чисел бесконечно много

▷ ∃ это не так. Тогда $\mathbb{P} = \{p_1, \dots p_n\}$. ∃ $m = p_1 \cdot \dots p_n + 1$, а q - наименьший собственный делитель m. Тогда по свву 2 $q \in \mathbb{P}$, значит $q = p_i$ для некоторого $i \in \{1, \dots n\}$. Так как $m - 1 : p_i$ $(m, p_i) = (1, p_i) = 1$ (по свву 2 НОДа). Значит, $m \not: p_i$, противоречие // q входит в то перемноженное число, тогда НОД $(m, p_i) = 1$, что противоречит перемножению. ◀

Билет 8

Основная теорема арифметики (Теорема 7)

$\forall a \in \mathbb{N}$, $a > 1$ раскладывается в произведение простых чисел. Такое разложение единственно с точностью до порядка сомножителей. // $a = p_1 \dots p_n$ - единств.

▷ По индукции. База $n \in \mathbb{P}$ очевидна: разложение $a = a$. Переход: ∃ a - составное, а для меньших чисел теорема доказана. Тогда $a = bc$, где $1 < b, c < a$, следовательно, $b = p_1 \cdot \dots p_n$ и $c = q_1 \cdot \dots q_m$, тогда $a = p_1 \cdot \dots p_n q_1 \cdot \dots q_m$ - искомое разложение.

Предположим противное, пусть $a = p_1 \cdot \dots p_n = q_1 \cdot \dots q_m$ - два разложения на простые, причём a - наименьшее натуральное, для которого разложение неединственно.

Из это следует, что $a = p_1 \cdot \dots p_n : q_1 \Rightarrow$ для какого-то $p_i : q$ верно. Но $p_i, q_1 \in \mathbb{P}$ и $p_i : q_1 \Rightarrow p_i = q_1$. Тогда $a' = \frac{a}{p_1} = p_2 \cdot \dots p_n = q_2 \cdot \dots q_m$. Но разложение a' в произведение простых единственно (по предположению индукции). ◀

Билет 9

Опр

Каноническое разложение - представление натурального числа в виде $n = p_1^{k_1} \cdot \dots p_s^{k_s}$, где $p_1 \dots p_s \in \mathbb{P}$ различны

Опр. для $n \in \mathbb{N}$ обозначим через $d(n)$ кол-во натуральных делителей n.

Теорема 8 (о кол-ве натур. делителей числа и о делителях числа)

∃ $n = p_1^{k_1} \cdots p_s^{k_s}$ - каноническое разложение. Тогда выполнены следующие условия: 1) $n \vdots d$, если и только если $d = p_1^{l_1} \cdots p_s^{l_s}$, где $0 \le l_i \le k_i$ для всех $i \in \{1, \dots s\}$.
2) $d(n) = (k_1+1) \cdots (k_s+1)$

▷ 1) $\Leftarrow$ Очевидно // достаточность

$\Rightarrow$ Если $n \vdots d$, то d не может иметь простых делителей, кроме $p_1, \dots p_s$ (по ОТА) $\Rightarrow d = p_1^{l_1} \cdots p_s^{l_s}$. Если $l_i > k_i$ для какого-то $i \in \{1, \dots s\}$, то очевидно, что $n \not\vdots d$. (по ОТА и делимости)

2) Показатель степени простого числа p_i в каноническом разложении делителя $d \mid n$ можно выбрать $k_i + 1$ способами $(0, \dots k_i)$. Перемножаем количество вариантов для различных p_i - profit! ◀

Билет 10

Теорема 9 (о представлении НОД через каноническое разложение)

∃ $a_1, \dots a_m \in \mathbb{N}$, $p_1, \dots p_s \in \mathbb{P}$ причём $a_i = p_1^{k_{i,1}} \cdots p_s^{k_{i,s}}$ для всех $i \in \{1, \dots m\}$ (некоторые из показателей могут быть равны 0). Тогда:

$$(a_1, \dots a_m) = p_1^{\min(k_{1,1}, \dots k_{m,1})} \cdots p_s^{\min(k_{1,s}, \dots k_{m,s})}$$

// по сути выбираем так, чтобы НОД имел каждую комбинацию множителей.

Пример:

$a_1 = 3 = 2^0 \cdot 3^1$

$a_2 = 4 = 2^2 \cdot 3^0$

$a_3 = 6 = 2^1 \cdot 3^1$

$a_4 = 8 = 2^3 \cdot 3^0$

$(a_1, a_2, a_3, a_4) = (3, 4, 6, 8) = 2^{\min(0,1,2,3)} \cdot 3^{\min(0,1)} = 2^0 \cdot 3^0 = 1$ - НОД чисел

▷ по теореме 8 (о кол-ве делителей $n \in \mathbb{N}$), $d \mid a_i$, если и только если $d = p_1^{l_1} \cdots p_s^{l_s}$, где $l_j \le k_{i,j}$ для всех $j \in \{1, \dots s\}$. $\Rightarrow d \in OD(a_1, \dots a_m)$, если и только если $d = p_1^{l_1} \cdots p_s^{l_s}$, где $l_i \le \min(k_{1,i} \dots k_{m,i})$ для $\forall i \in \{1, \dots s\}$. ◀

Билет 11

Вид диофантова уравнения: $ax+by=c$ (*) a,b,c - const, x,y - неизвестные $\in \mathbb{Z}$

- ∃ $d=(a,b)$. Если $c \vdots d$, то уравнение (*) решений не имеет.
- ∃ $c \vdots d$. Тогда введём замену: $a=da'$, $b=db'$, $c=dc'$

Тогда уравнение (*) эквивалентно $a'x+b'y=c'$, где $(a',b')=1$

Тогда ∃ линейное представление НОД: $a'x_0+b'y_0=1$. Умножив на c', получим $a'(x_0c')+b'(y_0c')=c$ // т.е. "по цепочке" умножаем найдённое, пока оно не встанет вместо исходного

Теорема 10

Решения уравнения (*) представляются в виде $x=x_0c'+tb'$, $y=y_0c'-ta'$, $t \in \mathbb{Z}$.

▷ Будем работать с эквивалентным уравнением $a'(x_0c')+b'(y_0c')=c'$.

Проверим, что $x=x_0c'+tb'$ и $y=y_0c'-ta$ действительно его решают: $a'(x_0c'+tb')+b'(y_0c'-ta')=a'(x_0c')+b'(y_0c')+a'tb'-b'ta'=c'$ - работает! // просто подставили, и оно сократилось

Проверим для исходного: $a'x+b'y=c'=a'(x_0c')+b'(y_0c') \Rightarrow a'(x-x_0c')=b'(y_0c'-y)$ (т.к. самая эквивалентность) (вынесли за скобки). Тогда $a'(x-x_0c') \vdots b'$ (по ОТА), т.к. $(a',b')=1$, то $x-x_0c' \vdots b'$. ∃ s (сократили $a=a'd$, $b=b'd$) $x-x_0c'=tb'$. Аналогично $y_0c'-y \vdots a'$. ∃ $y_0c'-y=sa'$. Тогда $a'tb'=b'sa'$, откуда $s=t$ (аналогично). // просто записали сокращенно

// сделали вывод, т.к. $(a',b')=1 \Rightarrow$ по ОТА можно и для других чисел.